

# MULTIPLICATIVE ENERGY OF SHIFTED SUBGROUPS AND BOUNDS ON EXPONENTIAL SUMS WITH TRINOMIALS IN FINITE FIELDS

SIMON MACOURT, ILYA D. SHKREDOV, AND IGOR E. SHPARLINSKI

**ABSTRACT.** We give a new bound on colinear triples in subgroups of prime finite fields and use it to give some new bounds on exponential sums with trinomials.

## 1. INTRODUCTION

**1.1. Set up.** For a prime  $p$ , we use  $\mathbb{F}_p$  to denote the finite field of  $p$  elements.

For a  $t$ -sparse polynomial

$$\Psi(X) = \sum_{i=1}^t a_i X^{k_i}$$

with some pairwise distinct non-zero integers exponents  $k_1, \dots, k_t$  and coefficients  $a_1, \dots, a_t \in \mathbb{F}_p^*$ , and a multiplicative character  $\chi$  of  $\mathbb{F}_p^*$  we define the sums

$$S_\chi(\Psi) = \sum_{x \in \mathbb{F}_p^*} \chi(x) \mathbf{e}_p(\Psi(x))$$

where  $\mathbf{e}_p(u) = \exp(2\pi i u/p)$  and  $\chi$  is an arbitrary multiplicative character of  $\mathbb{F}_p^*$ . The most interesting well-studied special case is when  $\chi = \chi_0$  is a principal character, however most of our results extend to the general case with any loss of strength of complication of the argument (as well as most of the previous results), so this is how we present them.

The main challenge here is to estimate these sums better than by the Weil bound

$$|S_\chi(\Psi)| \leq \max\{k_1, \dots, k_t\} p^{1/2},$$

see [36, Appendix 5, Example 12], by taking advantage of sparsity and also the arithmetic structure of the exponents  $k_1, \dots, k_t$ . For monomials  $\Psi(X) = aX^k$  (where we can always assume that  $k \mid p-1$ ) the first

---

2010 *Mathematics Subject Classification.* 11L07, 11T23.

*Key words and phrases.* exponential sum, sparse polynomial, trinomial.

bound of this type is due to Shparlinski [34] which has then been improved and extended in various directions by Bourgain, Glibichuk and Konyagin [7], Bourgain [3], Heath-Brown and Konyagin [19], Konyagin [22], Shkredov [27], Shteinikov [32].

Akulichev [1] gives several bounds on binomials, see also [38]. Cochrane, Coffelt and Pinner, see [9, 10, 11, 12, 13, 14] and references therein, have given a series of other bounds on exponential sums with sparse polynomials, some of which we present below in Section 1.2.

We also remark that exponential sums with sparse polynomials and a composite denominator have been studied in [4, 33].

Here we use a slightly different approach to improve some of the previous results. Our approach is related on reducing bounds of exponential sums with sparse polynomials to bounds of weighted multilinear exponential sums of the type considered in [25]. However, instead of applying the results of [25] directly, we first obtain their more precise version for triple weighted sums over multiplicative subgroups of  $\mathbb{F}_p^*$ , which could be of independent interest, see Lemma 3.4 below.

This result rests on an extension of the bound on the number of collinear triples from multiplicative subgroups from [28, Proposition 1] to subgroups of any size, see Theorem 1.1. In turn, this gives a new bound on the multiplicative energy of arbitrary subgroups, see Corollary 4.1, and has several other applications, see Section 4.

Although here we concentrate on the case of trinomials

$$(1.1) \quad \Psi(X) = aX^k + bX^m + cX^n,$$

our method works, without any changes, for more general sums with polynomials of the shape

$$\Psi(X) = aX^k + f(X^m) + g(X^n)$$

with arbitrary polynomials  $f, g \in \mathbb{F}_p[X]$  (uniformly in the degrees of  $f$  and  $g$ , which essentially means that they can be any functions defined on  $\mathbb{F}_p$ ).

One can certainly use our approach for sums with quadrinomials, using a version of [25, Theorem 1.3], using our Lemma 3.2 in an appropriate place. Furthermore, using results of [4, 6, 17], one can consider the case of arbitrary sparse polynomials.

The notation  $A \ll B$  is equivalent to  $|A| \leq c|B|$  for some constant  $c$ , which, throughout the paper may only depend on the number of monomials in the sparse polynomials under considerations.

**1.2. Previous results.** We compare our results for trinomials (1.1) with the estimates of Cochrane, Coffelt and Pinner [9, Equation (1.6)]

$$(1.2) \quad S_\chi(\Psi) \ll p^{7/8} \left( \frac{k\ell m}{\max\{k, \ell, m\}} \right)^{1/4}$$

which is non-trivial for  $\min\{k\ell, km, \ell m\} < p^{1/2}$ , and of Cochrane and Pinner [11, Theorem 1.1]:

$$(1.3) \quad S_\chi(\Psi) \ll p^{5/6} (k\ell m)^{1/9}$$

which is non-trivial for  $k\ell m < p^{3/2}$ , or  $\ell m < p^{1/2}$ .

We also recall the bound of Cochrane, Coffelt and Pinner [10, Corollary 1.1]

$$(1.4) \quad S_\chi(\Psi) \ll D^{1/2} p^{7/8} + (k\ell m)^{1/4} p^{5/8}$$

where  $D = \gcd(k, \ell, m, p-1)$ .

**1.3. New results.** For a set  $\mathcal{U} \subset \mathbb{F}_p^*$  we define  $T(\mathcal{U})$  to be number of solutions to

$$(1.5) \quad \frac{u_1 - v_1}{u_1 - w_1} = \frac{u_2 - v_2}{u_2 - w_2}, \quad u_i, v_i, w_i \in \mathcal{U}, \quad i = 1, 2.$$

As we relation (2.1) shows, the triples  $(u_i, v_i, w_i)$ ,  $i = 1, 2$  satisfying (1.5) defined there collinear points. Recent results on the quantity  $T(\mathcal{U})$  for an arbitrary set  $\mathcal{U}$  can be found in [23].

Note that in (1.5) as well as in all similar expressions of this type we consider only the values of the variables for which these expressions are defined (that is,  $u_i \neq w_i$ ,  $i = 1, 2$  in (1.5)).

We begin by providing a new result on the number of collinear triples in subgroups.

**Theorem 1.1.** *Let  $\mathcal{G}$  be a multiplicative subgroup of  $\mathbb{F}_p^*$ . Then*

$$T(\mathcal{G}) - \frac{|\mathcal{G}|^6}{p} \ll \begin{cases} p|\mathcal{G}|^3, & \text{if } |\mathcal{G}| \geq p^{3/4}, \\ |\mathcal{G}|^5 p^{-1/2}, & \text{if } p^{3/4} > |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^4 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

**Remark 1.2.** *Theorem 1.1 is new only for subgroups of size  $|\mathcal{G}| > p^{1/2}$ , otherwise it is contained in [28, Proposition 1].*

**Remark 1.3.** *Analysing the proof of Theorem 1.1, one see the Cartesian products  $\mathcal{G} \times \mathcal{G}$  can be replaced with the Cartesian products of different cosets of  $\mathcal{G}$  and also to variables  $u_i, v_i, w_i \in \lambda_i \mathcal{G}$ ,  $i = 1, 2$ , from two different cosets of  $\mathcal{G}$ .*

We obtain the following result on trinomial sums.

**Theorem 1.4.** *Let  $\Psi(X)$  be a trinomial of the form (1.1) with  $a \in \mathbb{F}_p^*$ . Define*

$$d = \gcd(k, p-1), \quad e = \gcd(\ell, p-1), \quad f = \gcd(m, p-1)$$

and

$$g = \frac{d}{\gcd(d, f)}, \quad h = \frac{e}{\gcd(e, f)}.$$

Suppose  $g \geq h$ , then

$$S_\chi(\Psi) \ll \begin{cases} p^{7/8} f^{1/8}, & \text{if } h \geq p^{1/2} \log p, \\ p^{15/16} (f/h)^{1/8+o(1)}, & \text{if } g \geq p^{1/2} \log p > h, \\ p(f/gh)^{1/8+o(1)}, & \text{if } g < p^{1/2} \log p. \end{cases}$$

We observe that the bound of Theorem 1.4 is independent of the size of our powers  $k$ ,  $\ell$  and  $m$  and is strongest for large  $d$  and  $e$  and small greatest common divisors  $f$ ,  $\gcd(d, f)$  and  $\gcd(e, f)$ . In particular, it may remain nontrivial even for polynomials of very large degrees, while the bounds (1.2), (1.3) and (1.4) all become trivial for trinomials of large degree. Thus it is easy to give various families of set of parameters when Theorem 1.4 improves the bounds (1.2), (1.3) and (1.4) simultaneously.

## 2. COLINEAR TRIPLES

**2.1. Preliminaries.** We require some previous results. The first one is a result of Mit'kin [24, Theorem 2] extending that of Heath-Brown and Konyagin [19, Lemma 5], see also [22, 26, 31] for further generalisations.

**Lemma 2.1.** *Let  $\mathcal{G}$  and  $\mathcal{H}$  be subgroups of  $\mathbb{F}_p^*$  and let  $\mathcal{M}_\mathcal{G} = \mathbb{F}_p^*/\mathcal{G}$  and  $\mathcal{M}_\mathcal{H} = \mathbb{F}_p^*/\mathcal{H}$  be the sets of distinct coset representatives of  $\mathcal{G}$  and  $\mathcal{H}$  in  $\mathbb{F}_p^*$ . For an arbitrary set  $\Theta \subset \mathcal{M}_\mathcal{G} \times \mathcal{M}_\mathcal{H}$  such that*

$$|\mathcal{G}|^2 |\mathcal{H}|^2 |\Theta| < p^3 \quad \text{and} \quad |\Theta| \leq |\mathcal{G}| |\mathcal{H}|,$$

we have

$$\sum_{(u,v) \in \Theta} |\{(x, y) \in \mathcal{G}^2 : ux + vy = 1\}| \ll (|\mathcal{G}| |\mathcal{H}| |\Theta|^2)^{1/3}.$$

We note that we use Lemma 2.1 only for  $\mathcal{G} = \mathcal{H}$ , however we present it in full generality as we believe the results has be known better.

Given a line

$$\ell_{a,b} = \{(x, y) \in \mathbb{F}_p^2 : y = ax + b\}$$

for some non-zero pair  $(a, b) \in \mathbb{F}_p^2$  and a set  $\mathcal{A} \subseteq \mathbb{F}_p$ , we denote  $\iota_\mathcal{A}(\ell_{a,b}) = |\ell_{a,b} \cap (\mathcal{A} \times \mathcal{A})|$ .

The following elementary identities are well-known and no doubt have appeared, implicitly and explicitly, in a number of works.

**Lemma 2.2.** *Let  $\mathcal{A} \subseteq \mathbb{F}_p$ . Then*

$$\sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b}) = p|\mathcal{A}|^2 \quad \text{and} \quad \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b})^2 = |\mathcal{A}|^4 - |\mathcal{A}|^3 + p|\mathcal{A}|^2.$$

*Proof.* The first relation is obvious as for every  $(x, y, a) \in \mathcal{A}^2 \times \mathbb{F}_p$  there is a unique  $b = y - ax$  counted in that sum.

For the second sum, we write

$$\begin{aligned} & \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b})^2 \\ &= \sum_{(u,v,x,y) \in \mathcal{A}^4} \#\{(a,b) \in \mathbb{F}_p^2 : v = au + b, y = ax + b\}. \end{aligned}$$

We now note that  $|\mathcal{A}|^2$  quadruples  $(u, v, x, y) \in \mathcal{A}^4$  with  $(u, v) = (x, y)$  define exactly  $p$  pairs  $(a, b) = (a, v - au) \in \mathbb{F}_p \times \mathbb{F}_p$ . Furthermore,  $|\mathcal{A}|^2(|\mathcal{A}| - 1)$  quadruples  $(u, v, x, y) \in \mathcal{A}^4$  with  $u = x$  but  $v \neq y$  do not define any pairs  $(a, b)$ . The remaining

$$|\mathcal{A}|^4 - |\mathcal{A}|^2(|\mathcal{A}| - 1) - |\mathcal{A}|^2 = |\mathcal{A}|^4 - |\mathcal{A}|^3$$

pairs define one pair  $(a, b) \in \mathbb{F}_p^2$  each, which concludes the proof.  $\square$

We now immediately derive

**Corollary 2.3.** *Let  $\mathcal{A} \subseteq \mathbb{F}_p$ . Then*

$$\sum_{(a,b) \in \mathbb{F}_p^2} \left( \iota_{\mathcal{A}}(\ell_{a,b}) - \frac{|\mathcal{A}|^2}{p} \right)^2 \leq p|\mathcal{A}|^2.$$

We now link  $T(\mathcal{G})$  with the quantities  $\iota_{\mathcal{G}}(\ell_{a,b})$ .

**Lemma 2.4.** *Let  $\mathcal{A} \subseteq \mathbb{F}_p$ . Then*

$$T(\mathcal{A}) = \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b})^3 + O(|\mathcal{A}|^4).$$

*Proof.* Transforming the equation (1.5) into

$$\frac{u_1 - v_1}{u_2 - v_2} = \frac{u_1 - w_1}{u_2 - w_2} \quad u_i, v_i, w_i \in \mathcal{U}, \quad i = 1, 2,$$

we introduce an error of magnitude  $O(|\mathcal{A}|^4)$  (coming from different pairs of variables which must be distinct). Then collecting, for every  $a \in \mathbb{F}_p$ , the solutions with

$$\frac{u_1 - v_1}{u_2 - v_2} = \frac{u_1 - w_1}{u_2 - w_2} = a$$

we derive:

$$u_1 - au_2 = v_1 - av_2 = w_1 - aw_2.$$

We now denoting this common value by  $b$  and observe that for any  $(a, b) \in \mathbb{F}_p^2$  there are  $\iota_{\mathcal{A}}(\ell_{a,b})^3$  solutions to

$$(2.1) \quad u_1 - au_2 = v_1 - av_2 = w_1 - aw_2 = b.$$

Summing over all pairs  $(a, b) \in \mathbb{F}_p^2$ , we obtain the result.  $\square$

Using the identity  $X^3 = X(X - Y)^2 + 2X^2Y - XY^2$  with  $X = \iota_{\mathcal{A}}(\ell_{a,b})$  and  $Y = |\mathcal{A}|^2/p$  we see that

$$\begin{aligned} \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b})^3 &= \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b}) \left( \iota_{\mathcal{A}}(\ell_{a,b}) - \frac{|\mathcal{A}|^2}{p} \right)^2 \\ &\quad + 2 \frac{|\mathcal{A}|^2}{p} \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b})^2 - \frac{|\mathcal{A}|^4}{p^2} \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b}). \end{aligned}$$

Combining this with Lemma 2.2 yields

$$\begin{aligned} \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b})^3 &= \frac{|\mathcal{A}|^6}{p} + \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b}) \left( \iota_{\mathcal{A}}(\ell_{a,b}) - \frac{|\mathcal{A}|^2}{p} \right)^2 - 2|\mathcal{A}|^5/p + 2|\mathcal{A}|^4. \end{aligned}$$

Hence using Lemma 2.4, we obtain

**Corollary 2.5.** *Let  $\mathcal{A} \subseteq \mathbb{F}_p$ . Then*

$$T(\mathcal{A}) - \frac{|\mathcal{A}|^6}{p} = \sum_{(a,b) \in \mathbb{F}_p^2} \iota_{\mathcal{A}}(\ell_{a,b}) \left( \iota_{\mathcal{A}}(\ell_{a,b}) - \frac{|\mathcal{A}|^2}{p} \right)^2 + O(|\mathcal{A}|^4).$$

Given two set  $\mathcal{U}, \mathcal{V} \subseteq \mathbb{F}_p$ , we define  $E^\times(\mathcal{U}, \mathcal{V})$  to be the *multiplicative energy* of  $\mathcal{U}$  and  $\mathcal{V}$ , that is, the number of solutions to

$$u_1 v_1 = u_2 v_2, \quad u_1, u_2 \in \mathcal{U}, \quad v_1, v_2 \in \mathcal{V}.$$

For  $\mathcal{U} = \mathcal{V}$  we also write

$$E^\times(\mathcal{U}) = E^\times(\mathcal{U}, \mathcal{U}).$$

It is easy to see that for a subgroup of  $\mathcal{G} \subseteq \mathbb{F}_p^*$  we have

$$(2.2) \quad T(\mathcal{G}) = |\mathcal{G}|^2 E^\times(\mathcal{G} - 1) = \sum_{g, h \in \mathcal{G}} E^\times(\mathcal{G} - g, \mathcal{G} - h).$$

Finally, we need the following bound which is a special case of [28, Proposition 1].

**Lemma 2.6.** *Let  $p$  be a prime number and let  $\mathcal{G}$  be a subgroup of  $\mathbb{F}_p^*$  with  $|\mathcal{G}| < p^{1/2}$ . Then*

$$T(\mathcal{G}) \ll |\mathcal{G}|^4 \log |\mathcal{G}|.$$

**2.2. Proof of Theorem 1.1.** Now we are ready to prove our main result. The arguments follows [28, 30].

First of all, note that Lemma 2.6 implies the required result provided  $|\mathcal{G}| < \sqrt{p}$ .

Let  $\mathcal{X}$  be the set of all multiplicative characters of  $\mathbb{F}_p^*$  and let  $\mathcal{X}^* = \mathcal{X} \setminus \{\chi_0\}$  be the set of all nonprincipal characters of  $\mathbb{F}_p^*$ , see [21, Chapter 3] for a background on characters.

Using the orthogonality of characters (and collecting together solutions with at one, thus at least two variables which are equal to 1) we write

$$\begin{aligned} E^\times(\mathcal{G} - 1) &= \sum_{u_1, u_2, u_3, u_4 \in \mathcal{G} \setminus \{1\}} \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \chi \left( \frac{(u_1 - 1)(u_2 - 1)}{(u_3 - 1)(u_4 - 1)} \right) + O(|\mathcal{G}|^2) \\ &= \frac{1}{p-1} \sum_{\chi \in \mathcal{X}} \left| \sum_{u \in \mathcal{G} \setminus \{1\}} \chi(u - 1) \right|^4 + O(|\mathcal{G}|^2) \\ &= \frac{|\mathcal{G}|^4}{p} + \frac{1}{p-1} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{u \in \mathcal{G}} \chi(u - 1) \right|^4 + O(|\mathcal{G}|^2) \end{aligned}$$

(we note that the condition  $u \neq 1$  can be dropped from the summation also a slight simplification in main term can be absorbed in the error term  $O(|\mathcal{G}|^2)$ ). Now for  $k = (p-1)/|\mathcal{G}|$  we have

$$(2.3) \quad \left| \sum_{u \in \mathcal{G}} \chi(u - 1) \right| = \frac{1}{k} \left| \sum_{x \in \mathbb{F}_p^*} \chi(x^k - 1) \right| \leq p^{1/2}$$

by the Weil bound on multiplicative character sums, see [21, Theorem 11.23]. Hence, using this bound and then the of characters one more time, we obtain

$$\frac{1}{p-1} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{u \in \mathcal{G}} \chi(u - 1) \right|^4 \ll \frac{p}{p-1} \sum_{\chi \in \mathcal{X}^*} \left| \sum_{u \in \mathcal{G}} \chi(u - 1) \right|^2 \ll p^2 |\mathcal{G}|.$$

which dominates the previous error term  $O(|\mathcal{G}|^2)$  and gives  $E^\times(\mathcal{G} - 1) = |\mathcal{G}|^4/p + O(p|\mathcal{G}|)$ . Thus, together with (2.2)

$$(2.4) \quad T(\mathcal{G}) = |\mathcal{G}|^2 \left( \frac{|\mathcal{G}|^4}{p} + O(p|\mathcal{G}|) \right) = \frac{|\mathcal{G}|^6}{p} + O(p|\mathcal{G}|^3)$$

This gives the desired result for  $|\mathcal{G}| > p^{3/4}$ .

Let  $\Delta \geq 3$  be a parameter to be chosen later. Using Corollary 2.5, we obtain

$$(2.5) \quad T(\mathcal{G}) - \frac{|\mathcal{G}|^6}{p} \ll |\mathcal{G}|^4 + \Delta |\mathcal{G}|^2 p + \Sigma,$$

where

$$\Sigma = \sum_{\substack{(a,b) \in \mathbb{F}_p^2 \\ \iota_{\mathcal{G}}(\ell_{a,b}) > \Delta}} \iota_{\mathcal{A}}(\ell_{a,b}) \left( \iota_{\mathcal{G}}(\ell_{a,b}) - \frac{|\mathcal{G}|^2}{p} \right)^2.$$

Clearly, the contribution to  $\Sigma$  from lines with  $ab = 0$ , is most  $|\mathcal{G}|^4$  as in this case it does not vanish only for either  $a \in \mathcal{G}$  or  $b \in \mathcal{G}$  and then we have  $\iota_{\mathcal{A}}(\ell_{a,b}) = |\mathcal{G}|$  and

$$\sum_{\substack{(a,b) \in \mathbb{F}_p^2 \\ ab=0}} \iota_{\mathcal{A}}(\ell_{a,b}) \left( \iota_{\mathcal{G}}(\ell_{a,b}) - \frac{|\mathcal{G}|^2}{p} \right)^2 = O(|\mathcal{G}|^4).$$

Thus

$$(2.6) \quad \Sigma = \Sigma^* + O(|\mathcal{G}|^4)$$

where

$$\Sigma^* = \sum_{\substack{(a,b) \in (\mathbb{F}_p^*)^2 \\ \iota_{\mathcal{G}}(\ell_{a,b}) > \Delta}} \iota_{\mathcal{A}}(\ell_{a,b}) \left( \iota_{\mathcal{G}}(\ell_{a,b}) - \frac{|\mathcal{G}|^2}{p} \right)^2.$$

Hence, we can assume below that  $i(l) \geq \Delta$  and have deal just with the remaining sum  $\Sigma$ .

Returning to (1.5), we see that the quantity  $T(\mathcal{G})$  equals the number of the solution to the equation

$$(2.7) \quad (u_1 - v_1)(u_2 - w_2) = (u_1 - w_1)(u_2 - v_2), \quad u_i, v_i, w_i \in \mathcal{G}, \quad i = 1, 2.$$

One can assume that the products in (2.7) are nonzero and  $u_1 \neq v_1$  because there are at most  $O(|\mathcal{G}|^4)$  such solutions, which can be absorbed in the error term in (2.5). Denote by  $\sigma$  the remaining number of the solutions.

Let, as before,  $\mathcal{M}_{\mathcal{G}} = \mathbb{F}_p^*/\mathcal{G}$  be set of distinct coset representatives of  $\mathcal{G}$  in  $\mathbb{F}_p^*$ . Take another parameter  $\tau \geq \Delta$  and put

$$\Theta_{\tau} = \{(\alpha, \beta) \in \mathcal{M}_{\mathcal{G}}^2 : |\{(x, y) \in \mathcal{G}^2 : \alpha x + \beta y = 1\}| \geq \tau\}.$$

In other words,  $\Theta_{\tau}$  is the set of  $(u, v) \in \mathcal{M}_{\mathcal{G}}^2$  for which the lines

$$(2.8) \quad \mathcal{L}_{\alpha, \beta} = \{(x, y) \in \mathbb{F}_p^2 : \alpha x + \beta y = 1\} = \ell_{-\alpha\beta^{-1}, \beta^{-1}}$$



have the intersection with  $\mathcal{G}^2$  at least

$$\iota_{\mathcal{G}}(\ell_{-\alpha\beta^{-1}, \beta^{-1}}) \geq \tau.$$

By Lemma 2.1, we have  $|\Theta_{\tau}|\tau \ll (|\mathcal{G}||\Theta_{\tau}|)^{2/3}$  provided

$$|\mathcal{G}|^4|\Theta_{\tau}| < p^3 \quad \text{and} \quad |\Theta_{\tau}| \leq |\mathcal{G}|^2.$$

Clearly, this immediately implies that for the set

$$\mathcal{Q}_{\tau} = \{(\alpha, \beta) \in (\mathbb{F}_p^*)^2 : |\{(x, y) \in \mathcal{G}^2 : \alpha x + \beta y = 1\}| \geq \tau\}$$

we have

$$(2.9) \quad |\mathcal{Q}_{\tau}| = |\mathcal{G}|^2|\Theta_{\tau}| \ll |\mathcal{G}|^4\tau^{-3}$$

provided  $|\mathcal{G}|^4|\Theta_{\tau}| < p^3$  and  $|\Theta_{\tau}| \leq |\mathcal{G}|^2$ .

Since  $|\mathcal{G}|^2 > p$ , we have

$$|\Theta_{\tau}| \leq |\mathcal{M}_{\mathcal{G}}|^2 = (p-1)^2/|\mathcal{G}|^{-2} \leq |\mathcal{G}|^{-2}$$

we see that the upper bound (2.9) for  $\mathcal{Q}_{\tau}$  holds provided the only condition  $|\mathcal{G}|^4|\Theta_{\tau}| < p^3$  satisfied. Suppose, in contrary, that  $|\Theta_{\tau}| > p^3/|\mathcal{G}|^4$ . Whence, the number of incidences between points of  $\mathcal{P} = \mathcal{G}^2$  and the lines  $\mathcal{L}_{\alpha, \beta}$  as above with  $(\alpha, \beta) \in \mathcal{Q}_{\tau}$  is at least

$$(2.10) \quad |\mathcal{Q}_{\tau}|\tau > p^3|\mathcal{G}|^{-2}\Delta.$$

On the other hand, by a classical result which holds over any field (see, for example [8, Corollary 5.2] or [37, Exercise 8.2.1]) the number of incidences for any set of points  $\mathcal{P}$  and a set of lines  $\mathcal{Q}_{\tau}$  is at most  $|\mathcal{Q}_{\tau}|^{1/2}|\mathcal{P}| + |\mathcal{Q}_{\tau}|$ . Hence

$$(2.11) \quad |\mathcal{Q}_{\tau}|\tau \leq |\mathcal{Q}_{\tau}|^{1/2}|\mathcal{P}| + |\mathcal{Q}_{\tau}|$$

and we obtain

$$(2.12) \quad |\mathcal{Q}_{\tau}|\tau^2 \ll |\mathcal{P}|^2 = |\mathcal{G}|^4.$$

Combining (2.10) and (2.12), we derive

$$(2.13) \quad p^3|\mathcal{G}|^{-2}\Delta < |\mathcal{Q}_{\tau}|\tau \ll |\mathcal{G}|^4\tau^{-1} \leq |\mathcal{G}|^4\Delta^{-1}.$$

Now taking

$$(2.14) \quad \Delta = c|\mathcal{G}|^3p^{-3/2},$$

for a sufficiently large constant  $c$  (and recalling that  $|\mathcal{G}| \geq p^{1/2}$ ), we see that (2.13) impossible.

Thus, for the above choice (2.14) of  $\Delta$  we have the desired condition  $|\mathcal{G}|^4|\Theta_{\tau}| < p^3$  for any  $\tau \geq \Delta$  and therefore the bound (2.9) holds,

We see from (2.8) that there is a one-to-one correspondence between the lines  $\ell_{a,b}$ ,  $(a,b) \in (\mathbb{F}_p^*)^2$  and the lines  $\mathcal{L}_{\alpha,\beta}$ ,  $(\alpha,\beta) \in (\mathbb{F}_p^*)^2$ . We now now define

$$\tau_j = e^j \Delta, \quad j = 0, 1, \dots, J.$$

Note that due to the choice of  $\Delta$  and the condition  $|\mathcal{G}| \geq p^{1/2}$  we have

$$\tau_j \geq \tau_0 = \Delta \gg |\mathcal{G}|^3 p^{-3/2}, \quad j = 0, 1, \dots, J.$$

Then, recalling the bound (2.9), we conclude that the contribution to  $\Sigma_*$  from the lines with  $\tau_{j+1} \geq \iota_{\mathcal{G}}(\ell_{a,b}) > \tau_j$  is bounded by

$$(2.15) \quad |\mathcal{Q}_{\tau_j}| \tau_{j+1} (\tau_{j+1} + |\mathcal{G}|^2/p)^2 \ll |\mathcal{Q}_{\tau_j}| \tau_{j+1}^3 \ll |\mathcal{G}|^4$$

Summing up (2.15) we obtain

$$\Sigma^* \ll J |\mathcal{G}|^4 \ll |\mathcal{G}|^4 \log |\mathcal{G}|.$$

Substituting this bound in (2.6) and combining it with (2.5), we obtain

$$T(\mathcal{G}) = \frac{|\mathcal{G}|^6}{p} + O(|\mathcal{G}|^5 p^{-1/2} + |\mathcal{G}|^4 \log |\mathcal{G}|)$$

in the range  $p^{3/4} > |\mathcal{G}| \geq p^{1/2}$ . Thus, together with (2.4) (for  $|\mathcal{G}| > p^{3/4}$ ) and Lemma 2.6 (for  $|\mathcal{G}| < p^{1/2}$ ) we conclude the proof.

**Remark 2.7.** *In principle, a stronger version of the classical incidence bound which is used (2.11) may lead to improvements of Theorem 1.1. However the range where such improvements are known are far away from the range which appears in our applications, see [35].*

### 3. TRINOMIAL SUMS

**3.1. Preliminaries.** We recall the following classical bound of bilinear sums, see, for example, [5, Equation 1.4] or [17, Lemma 4.1].

**Lemma 3.1.** *For any sets  $\mathcal{X}, \mathcal{Y} \subseteq \mathbb{F}_p$  and any  $\alpha = (\alpha_x)_{x \in \mathcal{X}}$ ,  $\beta = (\beta_y)_{y \in \mathcal{Y}}$ , with*

$$\sum_{x \in \mathcal{X}} |\alpha_x|^2 = A \quad \text{and} \quad \sum_{y \in \mathcal{Y}} |\beta_y|^2 = B,$$

*we have*

$$\left| \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \alpha_x \beta_y \mathbf{e}_p(xy) \right| \leq \sqrt{pAB}.$$

We define  $D_{\times}(\mathcal{U})$  to be the number of solutions of

$$(u_1 - v_1)(u_2 - v_2) = (u_3 - v_3)(u_4 - v_4), \quad u_i, v_i \in \mathcal{U}, \quad i = 1, 2, 3, 4,$$

and as before we define  $T(\mathcal{U})$  as the number of solutions to (1.5).

We now recall the following bound from [25, Lemma 2.7].

**Lemma 3.2.** *For any set  $\mathcal{U} \subset \mathbb{F}_p^*$  with  $|\mathcal{U}| = U$ , we have*

$$D_{\times}(\mathcal{U}) \ll U^2 T(\mathcal{U}) + U^6.$$

Combining Lemma 3.2 with Theorem 1.1 we obtain

$$D_{\times}(\mathcal{G}) \ll \frac{|\mathcal{G}|^8}{p} + \begin{cases} p|\mathcal{G}|^5, & \text{if } |\mathcal{G}| \geq p^{3/4}, \\ |\mathcal{G}|^7 p^{-1/2}, & \text{if } p^{3/4} > |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^6 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

Since for  $|\mathcal{G}| \geq p^{1/2}$  the first term dominates, this simplifies as

**Corollary 3.3.** *For a multiplicative subgroup  $\mathcal{G} \subset \mathbb{F}_p^*$ , we have*

$$D_{\times}(\mathcal{G}) \ll \begin{cases} |\mathcal{G}|^8 p^{-1}, & \text{if } |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^6 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

Substituting in Corollary 3.3 into the proof of [25, Theorem 1.3], we obtain the following result for trilinear sums over subgroups, which improves the general bound of [25, Theorem 1.3].

**Lemma 3.4.** *For any multiplicative subgroups  $\mathcal{F}, \mathcal{G}, \mathcal{H} \subseteq \mathbb{F}_p^*$  of cardinalities  $F, G, H$ , respectively, with  $F \geq G \geq H$  and weights  $\rho = (\rho_{x,y})$ ,  $\sigma = (\sigma_{x,z})$  and  $\tau = (\tau_{y,z})$  with*

$$\max_{(u,v) \in \mathcal{F} \times \mathcal{G}} |\rho_{u,v}| \leq 1, \quad \max_{(u,w) \in \mathcal{F} \times \mathcal{H}} |\sigma_{u,w}| \leq 1, \quad \max_{(v,w) \in \mathcal{G} \times \mathcal{H}} |\tau_{v,w}| \leq 1,$$

we have

$$\begin{aligned} & \sum_{u \in \mathcal{F}} \sum_{v \in \mathcal{G}} \sum_{w \in \mathcal{H}} \rho_{u,v} \sigma_{u,w} \tau_{v,w} \mathbf{e}_p(auvw) \\ & \ll \begin{cases} F^{7/8} GH, & \text{if } H \geq p^{1/2} \log p, \\ p^{1/16} F^{7/8} GH^{7/8+o(1)}, & \text{if } G \geq p^{1/2} \log p > H, \\ p^{1/8} F^{7/8} G^{7/8+o(1)} H^{7/8}, & \text{if } G < p^{1/2} \log p. \end{cases} \end{aligned}$$

uniformly over  $a \in \mathbb{F}_p^*$ .

*Proof.* We define

$$T = \sum_{x \in \mathcal{F}} \sum_{y \in \mathcal{G}} \sum_{z \in \mathcal{H}} \rho_{x,y} \sigma_{x,z} \tau_{y,z} \mathbf{e}_p(xyz)$$

and we see from [25, Equation (3.8)] that

$$T^8 \ll p F^7 G^4 H^4 K + F^8 G^8 H^6,$$

where  $K$  is the number of solutions to the equation

$$\begin{aligned} (u_1 - u_2)(w_1 - w_2) &= (u_3 - u_4)(w_3 - w_4) \neq 0, \\ (y_i, z_i) &\in \mathcal{G} \times \mathcal{H}, \quad i = 1, 2, 3, 4. \end{aligned}$$

As in the proof of [25, Theorem 1.3], expressing  $K$  via multiplicative character sums and using the Cauchy inequality, we obtain  $K^2 \leq D_\times(\mathcal{G})D_\times(\mathcal{H})$ . Applying Corollary 3.3, instead of [25, Equation 3.9], we now obtain

$$K \ll \begin{cases} G^4 H^4 / p, & \text{if } H \geq p^{1/2} \log p, \\ G^4 H^{3+o(1)} p^{-1/2}, & \text{if } G \geq p^{1/2} \log p > H, \\ (GH)^{3+o(1)}, & \text{if } G < p^{1/2} \log p. \end{cases}$$

We now deal with the three cases separately.

For  $H > p^{1/2} \log p$  we have

$$T^8 \ll F^7 G^8 H^8 + F^8 G^8 H^6.$$

Since for  $F \geq G \geq H$  the first term dominates, we obtain

$$(3.1) \quad T \ll F^{7/8} GH.$$

For  $G > p^{1/2} \log p > H$ , we have

$$T^8 \ll p^{1/2} F^7 G^8 H^7 \log H + F^8 G^8 H^6$$

or

$$(3.2) \quad T \ll p^{1/16} F^{7/8} GH^{7/8+o(1)} + FGH^{3/4}.$$

The first term of (3.2) dominates for  $p^{1/2} \geq F/H$ .

We now note that by Lemma 3.1 we also have

$$(3.3) \quad T \ll p^{1/2} F^{1/2} G^{1/2} H.$$

Furthermore, since for  $F > p^{1/2} H$  and  $G > p^{1/2}$  we have

$$\begin{aligned} p^{1/2} F^{1/2} G^{1/2} H &= p^{1/16} F^{7/8} GH^{7/8} \left( \frac{p^{7/2} H}{F^3 G^4} \right)^{1/8} \\ &< p^{1/16} F^{7/8} GH^{7/8} \left( \frac{p^3}{F^2 G^4} \right)^{1/8} < p^{1/16} F^{7/8} GH^{7/8}. \end{aligned}$$

we see that for  $G \geq p^{1/2} \log p > H$  the bound (3.2) simplifies as

$$(3.4) \quad T \leq p^{1/16} F^{7/8} GH^{7/8+o(1)}.$$

For  $G < p^{1/2} \log p$ , we have

$$T^8 \ll p F^7 G^{7+o(1)} H^{7+o(1)} + F^8 G^8 H^6$$

or

$$(3.5) \quad T \ll p^{1/8} F^{7/8} G^{7/8+o(1)} H^{7/8} + FGH^{3/4}.$$

The first term of (3.5) dominates for  $pH \geq FG$ . Otherwise, that is, for  $pH < FG$ , we have

$$\begin{aligned} p^{1/2} F^{1/2} G^{1/2} H &= p^{1/8} F^{7/8} G^{7/8} H^{7/8} \left( \frac{p^3 H}{F^3 G^3} \right)^{1/8} \\ &< p^{1/8} F^{7/8} G^{7/8} H^{7/8} \left( \frac{1}{H^2} \right)^{1/8} \leq p^{1/8} F^{7/8} G^{7/8} H^{7/8}. \end{aligned}$$

Thus, using (3.3) we see that for  $G < p^{1/2} \log p$ , the bound (3.5) simplifies as

$$(3.6) \quad T \leq p^{1/8} F^{7/8} G^{7/8+o(1)} H^{7/8}.$$

Combining (3.1), (3.4) and (3.6), we complete the proof.  $\square$

Clearly, the bound of Lemma 3.4 is nontrivial when  $F$ ,  $G$  and  $H$  are all a little large than  $p^{1/3}$ . More formally, for any  $\varepsilon > 0$  there exists some  $\delta > 0$  such that if  $F \geq G \geq H \geq p^{1/3+\varepsilon}$  then for the exponential sums of Lemma 3.4 we have

$$\sum_{u \in \mathcal{F}} \sum_{v \in \mathcal{G}} \sum_{w \in \mathcal{H}} \rho_{u,v} \sigma_{u,w} \tau_{v,w} \mathbf{e}_p(auvw) \ll FGH p^{-\delta}.$$

**3.2. Proof Theorem 1.4.** Let  $\mathcal{G}_d$  and  $\mathcal{G}_e$  be the subgroups of  $\mathbb{F}_p^*$  formed by the elements of orders  $d$  and  $e$ , respectively.

We have,

$$\begin{aligned} S_\chi(\Psi) &= \frac{1}{de} \sum_{y \in \mathcal{G}_d} \sum_{z \in \mathcal{G}_e} \sum_{x \in \mathbb{F}_p^*} \chi(xyz) \mathbf{e}_p(\Psi(xyz)) \\ &= \frac{1}{de} \sum_{x \in \mathbb{F}_p^*} \sum_{y \in \mathcal{G}_d} \sum_{z \in \mathcal{G}_e} \chi(x) \chi(y) \chi(z) \mathbf{e}_p(ax^k z^k + bx^\ell y^\ell + cx^m y^m z^m) \\ &= \frac{1}{de} \sum_{x \in \mathbb{F}_p^*} \sum_{z \in \mathcal{G}_e} \sum_{y \in \mathcal{G}_d} \rho_{x,y} \sigma_{x,z} \mathbf{e}_p(cx^m y^m z^m), \end{aligned}$$

where

$$\rho_{x,y} = \chi(x) \chi(y) \mathbf{e}_p(bx^\ell y^\ell) \quad \text{and} \quad \sigma_{x,z} = \chi(z) \mathbf{e}_p(ax^k z^k).$$

Clearly, the image  $\mathcal{X} = \{x^m : x \in \mathbb{F}_p^*\}$  contains  $(p-1)/f$  elements, each appearing with multiplicity  $f$ . Furthermore, direct examination shows that the images  $\mathcal{Y} = \{y^m : y \in \mathcal{G}_d\}$  and  $\mathcal{Z} = \{z^m : z \in \mathcal{G}_e\}$  contain  $g$  and  $h$  elements with multiplicities  $\gcd(d, f)$  and  $\gcd(e, f)$ , respectively. We recall that by our assumption we have  $g \geq h$

and revoke Lemma 3.4, which gives us,

$$\begin{aligned}
S_\chi(\Psi) &\ll \frac{f \gcd(d, f) \gcd(e, f)}{de} \times \\
&\quad \begin{cases} (p/f)^{7/8} gh, & \text{if } h \geq p^{1/2} \log p, \\ p^{1/16} (p/f)^{7/8} gh^{-7/8+o(1)}, & \text{if } g \geq p^{1/2} \log p > h, \\ p^{1/8} (p/f)^{7/8} g^{7/8+o(1)} h^{7/8}, & \text{if } g < p^{1/2} \log p, \end{cases} \\
&= \begin{cases} p^{7/8} f^{1/8}, & \text{if } h \geq p^{1/2} \log p, \\ p^{15/16} f^{1/8} \Delta^{1/8+o(1)}, & \text{if } g \geq p^{1/2} \log p > g, \\ p f^{1/8} g^{-1/8+o(1)} h^{-1/8}, & \text{if } g < p^{1/2} \log p. \end{cases}
\end{aligned}$$

This concludes the proof.

#### 4. FURTHER APPLICATIONS

**4.1. Additive properties of subgroups.** As usual, given a rational function

$$R(X_1, \dots, X_m) \in \mathbb{F}_p(X_1, \dots, X_m),$$

and  $m$  sets  $\mathcal{A}_1, \dots, \mathcal{A}_m \subseteq \mathbb{F}_p$ , we define the set

$$\begin{aligned}
R(\mathcal{A}_1, \dots, \mathcal{A}_m) \\
= \{R(a_1, \dots, a_m) : (a_1, \dots, a_m) \in (\mathcal{A}_1 \times \dots \times \mathcal{A}_m) \setminus \mathcal{P}_R\},
\end{aligned}$$

where  $\mathcal{P}_R$  is the set of poles of  $R$ .

We note that we have used  $\mathcal{A}^m$  for the  $m$ -fold Cartesian product rather than for the  $m$ -fold product-set of a set  $\mathcal{A}$ ; however neither of these notations is used in this section. We also remark that for a scalar  $\lambda \in \mathbb{F}_p$  we use the convention

$$\lambda \mathcal{A} = \{\lambda\} \cdot \mathcal{A} = \{\lambda a : a \in \mathcal{A}\},$$

to denote cosets of  $\mathcal{A} \subseteq \mathbb{F}_p$ .

Applying Theorem 1.1 to cosets of  $\mathcal{G}$  (see Remark 1.3) using a slight generalisation of (2.2) we obtains

**Corollary 4.1.** *Let  $\mathcal{G}$  be a multiplicative subgroup of  $\mathbb{F}_p^*$ . Then for any  $\lambda \in \mathbb{F}_p^*$ , we have*

$$E^\times(\mathcal{G} + \lambda) - \frac{|\mathcal{G}|^4}{p} \ll \begin{cases} p|\mathcal{G}|, & \text{if } |\mathcal{G}| \geq p^{3/4}, \\ |\mathcal{G}|^3 p^{-1/2}, & \text{if } p^{3/4} > |\mathcal{G}| \geq p^{1/2} \log p, \\ |\mathcal{G}|^2 \log |\mathcal{G}|, & \text{if } |\mathcal{G}| < p^{1/2} \log p. \end{cases}$$

Note that for  $|\mathcal{G}|/\sqrt{p \log p} \rightarrow \infty$ , Corollary 4.1 gives an asymptotic formula for  $E^\times(\mathcal{G} + \lambda)$ ; otherwise we only have an upper bound.

**Corollary 4.2.** *Let  $\mathcal{G}$  be a multiplicative subgroup of  $\mathbb{F}_p^*$ . Further for any  $\lambda, \mu \in \mathbb{F}_p^*$ , for the sets*

$$\mathcal{S}_1 = \mathcal{G} + \lambda\mathcal{G} + \mu\mathcal{G} \quad \text{and} \quad \mathcal{S}_2 = \left\{ \frac{u - \lambda}{v - \mu} : u, v \in \mathcal{G} \right\}$$

*we have*

$$p - |\mathcal{S}_\nu| \ll \begin{cases} p^3 |\mathcal{G}|^{-3}, & \text{if } |\mathcal{G}| \geq p^{3/4}, \\ p^{3/2} |\mathcal{G}|^{-1}, & \text{if } p^{3/4} > |\mathcal{G}| \geq p^{1/2} \log p, \\ p^2 |\mathcal{G}|^{-2} \log p, & \text{if } p^{1/2} \log p \geq |\mathcal{G}| > (p \log p)^{1/2}, \end{cases}$$

*and for  $|\mathcal{G}| \leq (p \log p)^{1/2}$  we have*

$$|\mathcal{S}_\nu| \gg \frac{|\mathcal{G}|^2}{\log |\mathcal{G}|},$$

*for  $\nu = 1, 2$ .*

*Proof.* By the Cauchy inequality we have

$$|\mathcal{S}_1| \geq |(\mathcal{G} + \lambda)(\mathcal{G} + \mu)| \geq \frac{|\mathcal{G}|^4}{\sqrt{E^\times(\mathcal{G} + \lambda)E^\times(\mathcal{G} + \mu)}}.$$

Hence, using Corollary 4.1, we derive the result for  $\mathcal{S}_1$ .

Similarly the Cauchy inequality again we also have

$$|\mathcal{S}_2| \geq \left| \frac{\mathcal{G} + \lambda}{\mathcal{G} + \mu} \right| \geq \frac{|\mathcal{G}|^4}{\sqrt{E^\times(\mathcal{G} + \lambda)E^\times(\mathcal{G} + \mu)}},$$

and again Corollary 4.1 yields the required result.  $\square$

In particular, Corollary 4.2 applies to  $\mathcal{S}_1 = \mathcal{G} + \mathcal{G} + \mathcal{G}$  and  $\mathcal{S}_1 = \mathcal{G} + \mathcal{G} - \mathcal{G}$ . We note, Corollary 4.2 also allows us to obtain the following version of the *Romanoff theorem* modulo almost all primes  $p$ .

**Corollary 4.3.** *For a fixed integer  $g$  with  $|g| \geq 2$ , and sufficiently large  $Q$ , for all but  $o(Q/\log Q)$  primes  $p \leq Q$  every residue class modulo  $p$  can be represented as  $\ell + g^k + g^m + g^n$  for a prime  $\ell < p$  and positive integers  $k, m, n \leq p - 1$ .*

*Proof.* We recall that by a special case of a result of Indlekofer and Timofeev [20, Corollary 6], for any fixed positive  $\alpha < 1$  all but  $o(Q/\log Q)$  primes  $p \leq Q$  the multiplicative order of  $g$  modulo  $p$  is at least  $p^{1/2} \exp((\log p)^\alpha)$ . For each of these primes, applying Corollary 4.2 to the set  $\mathcal{S}_1 = \mathcal{G} + \mathcal{G} + \mathcal{G}$  corresponding to the group  $\mathcal{G} \equiv \langle g \rangle \pmod{p}$  generated by  $g$  modulo  $p$ , we obtain

$$p - |\mathcal{S}_1| \ll p \exp(-(\log p)^\alpha) = o(p/\log p),$$

and by the prime number theorem we conclude the proof.  $\square$

We remark that a classical result of Erdős and Murty [15] can also be used in the proof of Corollary 4.3, however the bound of [20, Corollary 6] used in full strength allows to get better estimates on the size of the exceptional set, it this becomes important. Perhaps more recent results of Ford [16] can be used to get further improvements.

**Corollary 4.4.** *Let  $\mathcal{G}$  be a multiplicative subgroup of  $\mathbb{F}_p^*$ , and  $|\mathcal{G}| \geq p^\kappa$ , where  $\kappa > 10/17$ . Then for any  $\lambda \in \mathbb{F}_p^*$  we have*

$$\frac{\lambda\mathcal{G} - \mathcal{G}}{\mathcal{G} - \mathcal{G}} = \mathbb{F}_p.$$

*Proof.* For  $|\mathcal{G}| > p^{2/3}$ , proceeding as in the proof of the bound of (2.4), for any  $\xi \in \mathbb{F}_p^*$  we can write

$$\begin{aligned} & |\{\lambda u_1 - u_2 = \xi(v_1 - v_2) : u_i, v_i \in \mathcal{G}, i = 1, 2\}| \\ &= \frac{|\mathcal{G}|^4}{p} + \frac{1}{p} \sum_{a \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{G}} \mathbf{e}_p(a\lambda u) \right| \left| \sum_{u \in \mathcal{G}} \mathbf{e}_p(qu) \right| \left| \sum_{u \in \mathcal{G}} \mathbf{e}_p(a\xi u) \right|^2. \end{aligned}$$

Using well-known analogue of (2.3) for exponential sums see, for example [19, Equation (1)], which can be derived from the properties of Gauss sums, see [21, Section 3.4], we obtain

$$\begin{aligned} & \left| |\{u_1 - u_2 = a(v_1 - v_2) : u_i, v_i \in \mathcal{G}, i = 1, 2\}| - \frac{|\mathcal{G}|^4}{p} \right| \\ & < \sum_{a \in \mathbb{F}_p^*} \left| \sum_{u \in \mathcal{G}} \mathbf{e}_p(au) \right|^2 = p|\mathcal{G}| - |\mathcal{G}|^2. \end{aligned}$$

Hence, for  $|\mathcal{G}| > p^{2/3}$

$$\begin{aligned} & |\{u_1 - u_2 = \xi(v_1 - v_2) : u_i, v_i \in \mathcal{G}, i = 1, 2\}| \\ & > \frac{|\mathcal{G}|^4}{p} - p|\mathcal{G}| + |\mathcal{G}|^2 > |\mathcal{G}|^2. \end{aligned}$$

Therefore, there is a solution with  $v_1 \neq v_2$  which leads to a representation  $\xi = (u_1 - u_2)/(v_1 - v_2)$  for every  $a \in \mathbb{F}_p^*$ . The case of  $\xi = 0$  is trivial.

Hence we can now assume that  $|\mathcal{G}| \leq p^{2/3}$ . Put

$$\mathcal{Q} = \frac{\lambda\mathcal{G} - \mathcal{G}}{\mathcal{G} - \mathcal{G}} \quad \text{and} \quad \mathcal{R} = \frac{\lambda\mathcal{G} - 1}{\mathcal{G} - 1}.$$

Clearly,

$$0 \in \mathcal{R} \subseteq \mathcal{Q} \quad \text{and} \quad \mathcal{R}\mathcal{G} = \mathcal{Q}.$$



Thus if  $\mathcal{Q} \neq \mathbb{F}_p$ , then for some  $\xi \neq 0$  one has  $\mathcal{R} \cap \xi\mathcal{G} = \emptyset$ . Now we apply a slight generalisation of the main observation from [29], namely, the formula  $\mathcal{R} = 1 - \mathcal{R}$ . It gives us  $(1 - \xi\mathcal{G}) \cap \mathcal{R} = \emptyset$  and multiplying by  $\mathcal{G}$ , we obtain  $(\mathcal{G} - \xi\mathcal{G}) \cap \mathcal{Q} = \emptyset$ .

We now use an upper bound for the additive energy

$$E^+(\mathcal{G}) = |\{u_1 + v_1 = u_2 + v_2 : u_i, v_i \in \mathcal{G}, i = 1, 2\}|$$

of a multiplicative subgroup  $\mathcal{G}$  of order  $|\mathcal{G}| \leq p^{2/3}$ , namely,

$$E^+(\mathcal{G}) \ll |\mathcal{G}|^{31/13} p^{1/26} \log^{8/13} |\mathcal{G}|,$$

see [26, Theorem 7], and obtain

$$|\mathcal{G} - \xi\mathcal{G}| \gg \frac{|\mathcal{G}|^4}{E^+(\mathcal{G})} \gg |\mathcal{G}|^\eta p^{-1/26}$$

for any fixed  $\eta < 21/13$ . Hence, in view of Corollary 4.2, applied with  $\mu = 1$  and thus  $\mathcal{S}_2 = \mathcal{R}$  (and  $p^{2/3} \geq |\mathcal{G}| \geq p^\kappa > p^{1/2} \log p$ , provided that  $p$  is large enough), we obtain

$$|\mathcal{G}|^\eta p^{-1/26} \leq |\mathbb{F}_p \setminus \mathcal{Q}| \leq |\mathbb{F}_p \setminus \mathcal{R}| \ll p^{3/2} |\mathcal{G}|^{-1}$$

and the result follows.  $\square$

Not that some auxiliary results established in the proofs of [18, Theorems 1 and 2] can be reformulated as bounds on the size of the set  $(\mathcal{A} - \mathcal{A})(\mathcal{A} - \mathcal{A})$  for an arbitrary set  $\mathcal{A} \subseteq \mathbb{F}_p$ , we also refer to [2] for more recent results and further references.

#### ACKNOWLEDGEMENTS

The authors would like to thank Giorgis Petridis for his comments and suggestions.

During the preparation of this work, the third author was supported by the Australian Research Council Grant DP140100118.

#### REFERENCES

- [1] N. M. Akulinichev, ‘Estimates for rational trigonometric sums of a special type’, *Doklady Acad. Sci. USSR*, **161** (1965), 743–745 (in Russian).
- [2] A. Balog, ‘Another sum-product estimate in finite fields’, *Proc. Steklov Inst. Math.*, **280** (2013), Suppl. 2, S23–S29.
- [3] J. Bourgain, ‘Multilinear exponential sums in prime fields under optimal entropy condition on the sources’, *Geom. and Funct. Anal.*, **18** (2009), 1477–1502.
- [4] J. Bourgain, ‘Estimates of polynomial exponential sums’, *Israel J. Math.*, **176** (2010), 221–240.

- [5] J. Bourgain and M. Z. Garaev, ‘On a variant of sum-product estimates and explicit exponential sum bounds in prime fields’, *Math. Proc. Cambridge Phil. Soc.*, **146** (2009), 1–21.
- [6] J. Bourgain and A. Glibichuk, ‘Exponential sum estimates over a subgroup in an arbitrary finite field’, *J. D’Analyse Math.*, **115** (2011), 51–70.
- [7] J. Bourgain, A. A. Glibichuk and S. V. Konyagin, ‘Estimates for the number of sums and products and for exponential sums in fields of prime order’, *J. Lond. Math. Soc.*, **73** (2006), 380–398.
- [8] J. Bourgain, N.H. Katz and T. Tao, ‘A sum-product estimate in finite fields, and applications’, *Geom. Funct. Anal.*, **14** (2004), 27–57.
- [9] T. T. Cochrane, J. Coffelt and C. G. Pinner, ‘A further refinement of Mordell’s bound on exponential sums’, *Acta Arith.*, **116** (2005), 35–41.
- [10] T. T. Cochrane, J. Coffelt and C. G. Pinner, ‘A system of simultaneous congruences arising from trinomial exponential sums’, *J. Theorie des Nombres, Bordeaux.*, **18** (2006), 59–72.
- [11] T. Cochrane and C. Pinner, ‘An improved Mordell type bound for exponential sums’, *Proc. Amer. Math. Soc.*, **133** (2005), 313–320.
- [12] T. Cochrane and C. Pinner, ‘Using Stepanov’s method for exponential sums involving rational functions’, *J. Number Theory*, **116** (2006), 270–292.
- [13] T. Cochrane and C. Pinner, ‘Bounds on fewnomial exponential sums over  $\mathbb{Z}_p$ ’, *Math. Proc. Camb. Phil. Soc.*, **149** (2010), 217–227.
- [14] T. Cochrane and C. Pinner, ‘Explicit bounds on monomial and binomial exponential sums’, *Quart. J. Math.*, **62** (2011), 323–349.
- [15] P. Erdős and R. Murty, ‘On the order of  $a \pmod{p}$ ’, *Proc. 5th Canadian Number Theory Association Conf.*, Amer. Math. Soc., Providence, RI, 1999, 87–97.
- [16] K. Ford, ‘The distribution of integers with a divisor in a given interval’, *Ann. of Math.*, **168** (2008), 367–433.
- [17] M. Z. Garaev, ‘Sums and products of sets and estimates of rational trigonometric sums in fields of prime order’, *Russian Math. Surveys*, **65** (2010), 599–658 (Transl. from *Uspekhi Mat. Nauk*).
- [18] A. Glibichuk, ‘Combinational properties of sets of residues modulo a prime and the Erdős-Graham problem’, *Math. Notes*, **79** (2006), 356–365 (Transl. from *Matem. Zametki*).
- [19] D. R. Heath-Brown and S. V. Konyagin, ‘New bounds for Gauss sums derived from  $k$ th powers, and for Heilbronn’s exponential sum’, *Quart. J. Math.*, **51** (2000), 221–235.
- [20] H.-K. Indlekofer and N. M. Timofeev, ‘Divisors of shifted primes’, *Publ. Math. Debrecen*, **60** (2002), 307–345.
- [21] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
- [22] S. V. Konyagin, ‘Bounds of exponential sums over subgroups and Gauss sums’, *Proc. 4th Intern. Conf. Modern Problems of Number Theory and Its Applications*, Moscow Lomonosov State Univ., Moscow, 2002, 86–114 (in Russian).
- [23] B. Murphy, G. Petridis, O. Roche-Newton, M. Rudnev and I. D. Shkredov, ‘New results on sum-product type growth in positive characteristic’, *Preprint*, 2017.

- [24] D. A. Mit'kin, 'Estimation of the total number of the rational points on a set of curves in a simple finite field', *Chebyshevsky Sbornik*, **4** (2003), no.4, 94–102 (in Russian)
- [25] G. Petridis and I. E. Shparlinski, 'Bounds on trilinear and quadrilinear exponential sums', *J. d'Analyse Math.*, (to appear).
- [26] I. D. Shkredov, 'Some new inequalities in additive combinatorics', *Moscow J. Comb. and Number Theory*, **3** (2013), 425–475.
- [27] I. D. Shkredov, 'On exponential sums over multiplicative subgroups of medium size', *Finite Fields and Appl.*, **30** (2014), 72–87.
- [28] I. D. Shkredov, 'On tripling constant of multiplicative subgroups', *Integers*, **16** (2016), #A75.
- [29] I. D. Shkredov, 'Difference sets are not multiplicatively closed', *Discrete Analysis*, **17** (2016), 1–21.
- [30] I. D. Shkredov, 'Differences of subgroups in subgroups', *Integers* (to appear).
- [31] I. D. Shkredov and I. V. Vyugin, 'On additive shifts of multiplicative subgroups', *Mat. Sb.*, **203** (2012), 81–100 (in Russian).
- [32] Y. N. Shteinikov, 'Estimates of trigonometric sums over subgroups and some of their applications', *Matem. Zametki*, **98** (2015), 606–625 (in Russian).
- [33] I. E. Shparlinski, 'On exponential sums with sparse polynomials and rational functions', *J. Number Theory*, **60** (1996), 233–244.
- [34] I. E. Shparlinski, 'On bounds of Gaussian sums', *Matem. Zametki*, **50** (1991), 122–130 (in Russian).
- [35] S. Stevens and F. de Zeeuw, 'An improved point-line incidence bound over arbitrary fields', *Preprint*, 2016 (available from <http://arxiv.org/abs/1609.06284>).
- [36] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.
- [37] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge University Press, Cambridge, 2006.
- [38] H. B. Yu, 'Estimates for complete exponential sums of special types', *Math. Proc. Camb. Phil. Soc.*, **131** (2001), 321–326.

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,  
SYDNEY, NSW 2052, AUSTRALIA

*E-mail address:* s.macourt@student.unsw.edu.au

STEKLOV MATHEMATICAL INSTITUTE OF RUSSIAN ACADEMY OF SCIENCES,  
UL. GUBKINA 8, MOSCOW, RUSSIA, 119991, AND INSTITUTE FOR INFORMATION  
TRANSMISSION PROBLEMS OF RUSSIAN ACADEMY OF SCIENCES, BOLSHOY  
KARETNY PER. 19, MOSCOW, RUSSIA, 127994, AND MIPT, INSTITUTSKII PER.  
9, DOLGOPRUDNII, RUSSIA, 141701

*E-mail address:* ilya.shkredov@gmail.com

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF NEW SOUTH WALES,  
SYDNEY, NSW 2052, AUSTRALIA

*E-mail address:* igor.shparlinski@unsw.edu.au